

УДК 621.797:621.664

Кондратенко Н.Р.

Рудик О.А.

# ШТУЧНІ ІМУННІ СИСТЕМИ ТА ЇХ ВИКОРИСТАННЯ ДЛЯ ВИРІШЕННЯ РІЗНИХ ТИПІВ ЗАДАЧ

Вінницький національний технічний університет

## Анотація

У доповіді описано принцип роботи штучної імунної системи. Також розглянуто класи задач для рішення яких можуть бути використані відповідні системи задля обґрунтування доцільності використання штучної імунної системи для подальшої розробки засобу біометричної системи ідентифікації по особливостям клавіатурного почерку.

**Ключові слова:** Біометрична ідентифікація, штучна імунна система, клавіатурний почерк, афінність, розпізнавання образів.

## Abstract

The article describes the principle of the artificial immune system. Also, classes of problems for the solution of which the appropriate systems can be used to justify the feasibility of using an artificial immune system for further development of a means of biometric identification system on the features of keyboard writing.

**Keywords:** Biometric identification, artificial immune system, keyboard handwriting, affinity, pattern recognition

## Вступ

Натхненні біологічними імунними системами, протягом останнього десятиліття з'явилися штучні імунні системи. Багато дослідників розробляють і створюють моделі на основі імунної системи для різних областей застосування. Штучні імунні системи можна визначити як обчислювальну парадигму, яка спирається на теорію імунології, спостерігаються імунними функціями, принципами та механізмами[5].

З появою великих корпоративних систем в яких зберігаються величезні обсяги конфіденційних даних розподілених по різних обчислювальним системам з різними грифами доступності з'явилась необхідність розмежування прав доступу до інформації, а також ідентифікації користувачів[1] в системі. На сьогоднішній день ефективними системами розмежування доступу, що поєднують в собі найбільшу достовірність і зручність експлуатації, є системи, що використовують біометричні методи ідентифікації[2].

## Результати дослідження

Для початку розглянемо загальний принцип роботи штучної імунної системи у вигляді алгоритму, що входить до класу клональних алгоритмів відбору[5]:

На вході в систему - набір зразків для розпізнавання  $S$ ; на виході ми повинні отримати набір «розпізнавачів»  $M$ , які в подальшому будуть здатні класифікувати нові для системи зразки. Створюється випадковий набір антитіл  $A$ .

Далі, для кожного зразка з набору  $S$  відбувається наступне:

- визначається міра афінності (affinity - характеристика, яка визначає схожість генетичного набору антигену (зразка) і антитіла; в ШИС[6] визначається за допомогою математичних відстаней) з кожним конкретним антитілом з набору  $A$ ;
- антитіла з піднабору  $A$  з найвищою афінністю клонуються, причому число клонів кожного антитіла пропорційно його афінності;
- кожен клон піддається мутації (зміни атрибутів; ступінь залежить від цільової функції), після чого вся популяція клонів одного антитіла порівнюється з батьківським. Якщо після

мутації клон виявляється краще батьківського, то він замінює останній в наборі А. Копії антитіл з найвищою афінністю відправляються в набір М;

- п антитіл с найнижчою афінністю замінюються в наборі А на випадково згенеровані антитіла.

Існує ще три основні класи алгоритмів відбору, які використовують ШС:

- Негативні алгоритми відбору, засновані на принципі позитивної і негативної селекції. Застосовуються ці методи, наприклад, для класифікації і розпізнавання аномалій у даних.
- Імунні мережеві алгоритми використовують структуру мережевого графа, де вузли - це віднайдені антитіла, а в ході алгоритму навчання відстань між ними зростає або скорочується в залежності від ступеня їх умовної «близькості». Така структура методу дозволяє використовувати його для вирішення завдань кластеризації, візуалізації даних і навіть для розробки штучних нейронних мереж.
- Дендритні алгоритми засновані на моделі дендритних клітини - ще одного виду імунокомпетентних клітин.

В цілому, ШС дозволяють вирішувати велику кількість завдань, особливо, пов'язаних з даними - крім класифікації і кластеризації, ШС здатна знаходити аномалії, розпізнавати образи і сигнали, моделювати системи пошуку і оптимізації, а також системи комп'ютерної безпеки.

Задача ідентифікації користувача за клавіатурним почерком[3] можна представити як задачу розпізнавання образу, так як часові інтервали між натисканням клавіш на клавіатурі і час утримання (натискання) клавіші дозволяють достатньо однозначно охарактеризувати почерк роботи користувача на клавіатурі і є унікальними для кожної людини. В даному випадку набір часових характеристики користувача виступає в ролі набору зразків для розпізнавання.

### Висновки

Порівняння характеристик клавіатурного почерку може відбуватися з використанням імовірнісно-статистичних методів, гістаграмного методу і за допомогою нейронних мереж[4]. Нейромережевий підхід добре зарекомендував себе для рішення задач пов'язаних з розв'язанням рівнянь великої розмірності, проте такий різновид нейроподібної мережі як штучна імунна система дозволить краще розпізнавати образ користувача серед інших користувачів, за рахунок особливостей даних систем, зокрема принципу афінності.

### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Защита программного обеспечения: Пер. с англ./ Д. Гроувер, Р.Сатер, Дж. Фипс и др./ Под редакцией Д. Гроувера. – М.: Мир, 1992.
2. В.Ф. Гузик, Г.А. Галуев, М.Н. Десятерик Биометрические системы идентификации личности – 2001.
3. Кен Філліпс. біометрія освоює корпоративний ринок // PC WEEK/RE 17 червня 1997.
4. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: Издательство Пенз. гос. ун-та, 2000.
5. Анатомия человека / Э.П. Борзяк, В.Я. Бочаров, Л.И. Волкова и др.: под ред. М.П. Сапина. – М.: Медицина, 1987.
6. Уоссермен Ф. Нейрокомпьютерная техника: теория и практика: Пер. с англ. – М.: Мир, 1992.
7. Азарова, А. О., Карпінець, В. В. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи”

**Рудик Олександр Анатолійович** — студент групи БС-146, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: alex08811@gmail.com

Науковий керівник: **Кондратенко Наталія Романівна** — канд. техн. наук, професор кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

***Rudyk Oleksandr A.*** — Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: alex08811@gmail.com

Supervisor: ***Kondratenko Natalia R.*** — Cand. Sc. (Eng), Professor of Cybersecurity, Vinnytsia National Technical University, Vinnytsia